(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
9. Februar 2006 (09.02.2006)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2006/013121 A1

(51) Internationale Patentklassifikation[7]: G07C 5/08, G07F 7/10

(21) Internationales Aktenzeichen: PCT/EP2005/052530

(22) Internationales Anmeldedatum: 2. Juni 2005 (02.06.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 037 801.0 3. August 2004 (03.08.2004) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: LINDINGER, Andreas [DE/DE]; Im Winkel 12, 78658 Flözlingen (DE). SALM, Michael [DE/DE]; Sommerbergstrasse 34 a, 78112 Peterzell (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, 80506 München (DE).

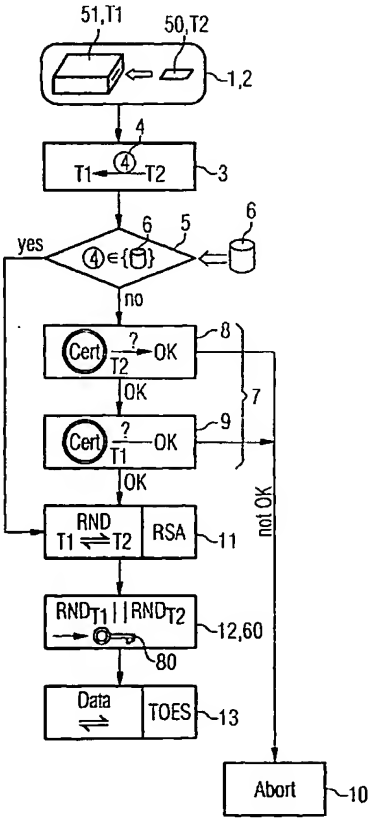
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR SECURELY TRANSMITTING DATA

(54) Bezeichnung: VERFAHREN ZUR SICHEREN DATENÜBERTRAGUNG



(57) Abstract: The invention relates to a method for securely transmitting data, particularly between a tachograph (51) of a goods-carrying vehicle and memory cards (50). A first node (T1) comprises a memory (6, 22) with entries (31-35) containing identifiers (4) and security certificates (Cert) of second nodes (T2). Methods for securely transmitting data are increasingly gaining importance and are often accompanied by a high amount of computing. As a result, the aim of the invention is to reduce the computing time without forfeiting security. To this end, the first node (T1) obtains an identifier (4) from the second node (T2) and compares it with stored identifiers (4). In the event of a matching identifier (4), a security certificate (Cert) assigned to this identifier (4) is provided as a basis for a subsequent data transmission, and in the event the identifier (4) does not match, a security certificate verification is carried out.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur sicheren Datenübertragung, insbesondere zwischen einem Fahrtschreiber (51) eines Nutzfahrzeuges und Speicherkarten (50), wobei ein erster Teilnehmer (T1) einen Speicher (6, 22) mit Einträgen (31-35) umfassend Kennungen (4) und Sicherheitszertifikate (Cert) zweiter Teilnehmer (T2) aufweist. Verfahren zur sicheren Datenübertragung gewinnen zunehmend an Bedeutung und gehen häufig mit hohem Rechenaufwand einher. Daher hat es sich die Erfindung zur Aufgabe gemacht, die Rechenzeit hierfür ohne Sicherheitseinbuße zu reduzieren. Es wird vorgeschlagen, dass der erste Teilnehmer (T1) von dem zweiten Teilnehmer (T2) eine Kennung (4) einholt und mit gespeicherten Kennungen (4) vergleicht. Bei übereinstimmender Kennung (4) ist ein dieser Kennung (4) zugeordnetes Sicherheitszertifikat (Cert) Basis für eine nachfolgende Datenübertragung und wenn keine über einstimmende Kennung (4) vorliegt wird eine Sicherheitszertifikatsverifikation durchführt.

WO 2006/013121 A1

GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Verfahren zur sicheren Datenübertragung

Die Erfindung betrifft ein Verfahren zur sicheren Datenübertragung zwischen einem ersten Teilnehmer und zweiten Teilnehmern, insbesondere einem Fahrtschreiber eines Nutzfahrzeuges und Speicherkarten mit jeweils mindestens einem Datenspeicher, wobei der erste Teilnehmer einen Speicher aufweist, in welchem eine bestimmte Anzahl Einträge gespeichert sind, jeweils umfassend Kennungen und zu diesem zugeordnete Sicherheitszertifikate zweiter Teilnehmer mit einer Erfassungszeit des Sicherheitszertifikates.

Verfahren zur sicheren Datenübertragung gewinnen zunehmend an Bedeutung und existieren bereits in umfassender Vielfalt im Bereich von Computernetzwerken. Im weiteren Sinne vergleichbar mit modernen Computernetzwerken ist auch das Zusammenwirken bzw. die sichere Datenübertragung eines digitalen Fahrtschreibers mit einer Speicherkarte gemäß der EG-Verordnung 3821/85. Zur Gewährleistung der Einhaltung bestehender Sozialvorschriften und Gesetze am Arbeitsplatz des Nutzfahrzeuges ist die Erhöhung der Manipulationssicherheit von besonderer Bedeutung. Daher werden strengste Maßstäbe an die Sicherheit der Datenübertragung gelegt. Hierzu ist ein System von Sicherheitszertifikaten umfassend verschiedene öffentliche und private Schlüssel entwickelt worden, welches im Einzelnen der vorgenannten Verordnung entnehmbar ist. Bevor ein erster Teilnehmer bzw. der Fahrtschreiber mit einem zweiten Teilnehmer bzw. einer Speicherkarte in einen Datenaustausch eintreten kann, ist unter anderem ein sehr aufwendiges Verfahren der Sicherheitszertifikatsverifikation auf beiden Seiten der Teilnehmerschaft erforderlich. Der Umfang dieses Vorgangs und

die eingeschränkten Möglichkeiten der Datenverarbeitung in dem kleinformatigen Gerät machen besondere Vorkehrungen erforderlich, damit die Zugriffszeiten bei akzeptablem Kostenaufwand in einem vernünftigen Rahmen bleiben.

Daher hat es sich die Erfindung zur Aufgabe gemacht, den insbesondere zeitlichen Aufwand der Sicherheitszertifikatsverifikationen für die Teilnehmer des Datenaustauschs ohne Einbußen der Manipulationssicherheit zu reduzieren.

Zur Lösung der Aufgabe wird erfindungsgemäß ein Verfahren der eingangs genannten Art vorgeschlagen, bei welchem vorgesehen ist, dass der erste Teilnehmer von dem zweiten Teilnehmer eine Kennung einholt, der erste Teilnehmer diese Kennung mit den in dem Speicher gespeicherten Kennungen vergleicht, wenn eine übereinstimmende Kennung in dem Speicher gespeichert ist, dass dieser Kennung zugeordnete Sicherheitszertifikat Basis für eine nachfolgende Datenübertragung ist und die Erfassungszeit des Sicherheitszertifikates auf eine aktuelle Systemzeit aktualisiert wird, wenn keine übereinstimmende Kennung in dem Speicher gespeichert ist, der erste Teilnehmer eine Sicherheitszertifikatsverifikation mit dem zweiten Teilnehmer durchführt und bei Verifizierung einen dem verifizierten Sicherheitszertifikat entsprechenden Eintrag mit aktueller Erfassungszeit in dem Speicher speichert, wobei der Eintrag mit dem ältesten Erfassungsdatum durch diesen neuen Eintrag ersetzt wird, wenn die bestimmte Anzahl an Einträgen schon erreicht war.

Ein entscheidender Vorteil des erfindungsgemäßen Verfahrens liegt in der Einsparung des sehr zeitaufwendigen Vorganges der Sicherheitszertifikatsverifikation für den Fall, dass dem ersten Teilnehmer der zweite Teilnehmer auf Grund eines in

der Vergangenheit bereits durchgeführten Verifikationsvorganges bekannt ist. Aus Speicherplatzgründen, insbesondere bei der Ausbildung des ersten Teilnehmers als Fahrtschreiber und des zweiten Teilnehmers als Speicherkarte, ist eine Begrenzung der Anzahl der Einträge umfassend die Sicherheitszertifikate und die Erfassungszeit der Sicherheitszertifikate anderer Teilnehmer begrenzt. Um trotz dieser Begrenzung das "Erinnerungsvermögen" des ersten Teilnehmers an zweite Teilnehmer auf eine Höchstanzahl an zweiten Teilnehmern zu optimieren, sieht das erfindungsgemäße Verfahren nicht eine einfache Ringspeicherung in chronologischer Abfolge des Auftretens der zweiten Teilnehmer vor, so dass stets beispielsweise der älteste Eintrag mit dem neuesten Eintrag überschrieben wird, wenn eine speicherplatzbedingte Höchstzahl an Einträgen schon erreicht war. Statt dessen wird zunächst der Inhalt des Speichers des ersten Teilnehmers daraufhin überprüft, ob bereits ein Eintrag mit identischer Kennung zu derjenigen des neuen Teilnehmers existiert, der im bejahenden Fall lediglich hinsichtlich des Erfassungsdatums und gegebenenfalls hinsichtlich des Ablaufs der Gültigkeit des Sicherheitszertifikates aktualisiert wird. Auf diese Weise sind dem ersten Teilnehmer, vorausgesetzt es wurde in der Vergangenheit bereits eine die bestimmte Anzahl an Speichereinträgen übersteigende Anzahl unterschiedlicher zweiter Teilnehmer verifiziert, stets die bestimmten Anzahl an zweiten Teilnehmern bekannt. Auf diese Weise kann die bestimmte Anzahl entsprechend den Gepflogenheiten beispielsweise eines Fuhrparks an die Anzahl der dort tätigen oder üblicherweise mit dem Nutzfahrzeug arbeitenden unterschiedlichen Karteninhaber angepasst werden und so eine optimale Nutzung des Speichers des ersten Teilnehmers erreicht werden. Die Zugriffszeiten bleiben vorteilhaft kurz, da auch bei wiederholtem Trennen und Verbinden des ersten Teilnehmers und des zweiten Teilnehmers stets nur die

der Identität des ersten Teilnehmers zugeordneten Einträge verändert bzw. aktualisiert werden.

Mit Vorteil ist die zur Identifizierung übermittelte Kennung der Teilnehmer ein öffentlicher Schlüssel eines RSA-Verfahrens (Verfahren zum Ver- und Entschlüsseln nach Ronald L. Rivest, Adi Schamir und Leonard Adleman) des zweiten Teilnehmers ist. Dieser öffentliche Schlüssel kann einerseits einer nachträglichen Datenübermittlung dienen und ist andererseits eindeutig.

Aus Gründen der Ersparnis von Rechenaufwand sieht eine vorteilhafte Weiterbildung vor, dass eine nachfolgende Datenübertragung mittels einer symmetrischen Verschlüsselung, insbesondere eines Triple-DES-Verfahrens erfolgt, wobei nach erfolgter Verifizierung der Sicherheitszertifikate beide Teilnehmer eine Zufallszahl verschlüsselt an den anderen Teilnehmer übersenden und beide Teilnehmer jeweils unabhängig voneinander mittels der beiden Zufallszahlen einen gemeinsamen Schlüssel zur Datenübertragung unter Benutzung desselben Algorithmus bestimmen. Im Wesentlichen bleibt hierbei die Sicherheit des asymmetrischen Verschlüsselungsverfahrens erhalten, da die Generierung des Sitzungsschlüssels für das symmetrische Verfahren nur demjenigen möglich ist, der zuvor mittels des asymmetrischen Verfahrens in der Lage war, mit dem anderen Teilnehmer zu kommunizieren bzw. die wechselseitig übermittelte Zufallszahl zu dechiffrieren.

Eine wichtige Position hinsichtlich der Manipulationssicherheit übernimmt gemäß dem Verfahren nach der Erfindung die Verifikation der Sicherheitszertifikate durch den jeweils anderen Teilnehmer, weshalb diese zweckmäßig folgende n Schritte umfasst:

In einem ersten Schritt übersendet der zweite Teilnehmer dem ersten Teilnehmer ein erstes Sicherheitszertifikat, welches der zweite Teilnehmer unter Benutzung eines ersten öffentlichen Schlüssels einer Verifizierung unterzieht und hierbei einen zweiten öffentlichen Schlüssel ermittelt. Resultiert die Verifizierung in Authentizität des übermittelten Sicherheitszertifikates, wird der erste Schritt unter Verwendung eines weiteren übersendeten Sicherheitszertifikates und des im vorhergehenden Schritt ermittelten zweiten öffentlichen Schlüssels anstelle des ersten öffentlichen Schlüssels (n-1)-fach wiederholt, wobei sich stets ein neuer zweiter öffentlicher Schlüssel und ein Verifizierungsergebnis ergibt. Diese verschachtelte Verifizierung kann zweckmäßig 3(=n)-fach wiederholt werden, was eine sehr hohe Manipulationssicherheit zum Ergebnis hat.

In der Folge ist die Erfindung anhand eines speziellen Ausführungsbeispiels unter Bezugnahme auf Zeichnungen zur Verdeutlichung näher beschrieben. Es zeigen:

Figur 1 eine schematische Darstellung des erfindungsgemäßen Verfahrens in Form eines Flussdiagramms,

Figur 2 ein Flussdiagramm des Vorgangs der Sicherheitszertifikatsverifizierung,

Figur 3 Einträge bekannter zweiter Teilnehmer in einem Speicher eines ersten Teilnehmers.

Das Flussdiagramm der Figur 1 zeigt beispielhaft wesentliche Züge des Ablaufes eines erfindungsgemäßen Verfahrens an einem Datenaustausch zwischen einem digitalen Fahrtschreiber 51 und einer Speicherkarte 50.

Das einleitende Ereignis 1 besteht in der Aufnahme 2 der Speicherkarte 50 mittels des Fahrtschreibers 51. Im Rahmen der Aufnahme 2 der Speicherkarte 50, welche im erfindungsgemäßen Sinne ein zweiter Teilnehmer T2 ist, stellt der Fahrtschreiber, welcher im erfindungsgemäßen Sinne ein erster Teilnehmer T1 ist, eine leitende Verbindung zu einem Datenspeicher der Speicherkarte 50 her, mittels derer Datensignale übertragbar sind.

In einem zweiten Schritt 3 holt der Fahrtschreiber 51 als erster Teilnehmer T1 von der Speicherkarte 50 als zweiten Teilnehmer T2 eine Kennung 4 ein und überprüft in einem dritten Schritt 5, ob die Kennung 4 bereits aus einem vorhergehenden Vorgang bekannt ist. Hierzu greift der Fahrtschreiber 51 auf einen integrierten Speicher 6 zu, in welchem Einträge mit in Figur 3 näher beschriebenem Umfang abgelegt sind.

Ist im Speicher 6 kein mit der Kennung 4 der Speicherkarte 50 abgelegter Eintrag vorhanden, geht das erfindungsgemäße Verfahren zu einer wechselseitigen Sicherheitszertifikatsverifikation 7 über. Hierbei werden während einer ersten Sicherheitszertifikatsverifikation Sicherheitszertifikate der Speicherkarte 50 mittels des Fahrtschreibers auf Gültigkeit, Bekanntheit und Authentizität gemäß Figur 2 überprüft, und anschließend findet eine entsprechende zweite Überprüfung 9 des Fahrtschreibers 51 seitens der Speicherkarte 50 statt.

Die Schritte 8 und 9 werden übersprungen, wenn im Schritt 5 der zweite Teilnehmer T2 bzw. die Speicherkarte 50 seitens des ersten Teilnehmers T1 als bekannt identifiziert wurde. Ist das endgültige Ergebnis einer Sicherheitszertifikatsverifikation gemäß der Schritt 8, 9 die Nicht-Verifikation, wird

die Speicherkarte 50 bzw. der erste Teilnehmer T1 in einem Schritt 10 ausgegeben bzw. abgewiesen.

Bei erfolgreicher wechselseitiger Verifikation bzw. bekannter Kennung 4 folgt in einem Schritt 11 ein wechselseitiger Austausch einer Zufallszahl in RSA-verschlüsselter Form, mittels derer in einem Schritt 12 ein gemeinsamer Sitzungsschlüssel 60 von beiden Teilnehmern T1, T2 unabhängig generiert wird, der im nachfolgenden Schritt 13 der symmetrischen Verschlüsselung übertragener Daten dient.

In Figur 2 ist die Sicherheitszertifikatsverifikation gemäß der Schritte 8, 9 in Figur 1 im Detail dargestellt. In einem ersten Schritt 21 holt der zweite Teilnehmer T2 von dem ersten Teilnehmer T1 ein Sicherheitszertifikat Cert.Lev.1 der ersten Ebene ein. Anhand von Einträgen eines Speichers 22 wird in einem zweiten Schritt 23 überprüft, ob der öffentliche Schlüssel oder eine Kennung des Sicherheitszertifikats Cert.Lev.1 der ersten Ebene bereits bekannt und noch gültig ist. Für den Fall der Gültigkeit und Bekanntheit geht das dargestellt Verfahren direkt zu einem Schritt 24 über, währenddessen der erste Teilnehmer T1 das Sicherheitszertifikat des zweiten Teilnehmers T2 in gleicher, nicht mehr gesondert dargestellter Weise einer Überprüfung unterzieht. Ist der öffentliche Schlüssel des Sicherheitszertifikats Cert.Lev.1 der Ebene 1 in dem Schritt 23 als nicht bekannt identifiziert worden, holt der zweite Teilnehmer T2 von dem ersten Teilnehmer T1 ein Sicherheitszertifikat Cert.Lev.2 der Ebene 2 in einem nachfolgenden Schritt 25 ein. Entsprechend dem Schritt 23 folgt in analoger Weise ein Schritt 26, währenddessen der zweite Teilnehmer T2 unter Zugriff auf den Speicher 22 die Bekanntheit und Gültigkeit eines öffentlichen Schlüssels des Sicherheitszertifikats Cert.Lev.2 der Ebene 2 überprüft. Ist

das Ergebnis der Überprüfung Bestätigung der Bekanntheit und Gültigkeit, geht das Verfahren direkt zu einem Verifizierungsschritt 27 über, währenddessen das Sicherheitszertifikat Cert.Lev.1 Ebene 1 einer Verifizierung unterzogen wird. Ist der öffentliche Schlüssel des Sicherheitszertifikats Cert.Lev.2 der Ebene 2 nicht bekannt und gültig, folgt zunächst die Verifizierung des Sicherheitszertifikats Cert.Lev.2 der Ebene 2 in einem Schritt 28, bevor die Verifizierung gemäß Schritt 27 eingeleitet wird. Haben die Überprüfungen der Schritte 27 und 28 Verifizierung der Sicherheitszertifikate Cert.Lev.1,2 der Ebene 1 und Ebene 2 zum Ergebnis, geht das Verfahren zum Schritt 24 über, welches eine bezüglich der Teilnehmer T1 und T2 umgekehrte Sicherheitszertifikatsverifikation einleitet.

Die Figur 3 zeigt den Inhalt des Speichers 22 bzw. 6 in Abhängigkeit eines Kommunikationseintrittes verschiedener zweiter Teilnehmer T2 mit einem ersten Teilnehmer T1. Die Größe des Speichers 6, 22 ist auf fünf Einträge 31-35 begrenzt. Es sind sechs aufeinander folgende Zustände 41-46 in Figur 3 abgebildet, die jeweils die Einträge 31-34 nach bestimmten Ereignissen wiedergeben. Die dargestellten Einträge 31-34 umfassen ein Datum 51, dessen Wert in hexadezimaler Schreibweise als Wert in Sekunden seit dem 1.1.1970 abgelegt ist. Daneben umfassen die Einträge 31-35 einen Sicherheitszertifikatsinhalt 52, der einen Ablauf EOV der Gültigkeit des Sicherheitszertifikats und eine Referenz CHR des Sicherheitszertifikatinhabers umfasst. Daneben umfassen die Einträge 31-35 auch die Erfassungszeit 53.

Der Zustand 41 zeigt den Ausgangszustand, der charakterisiert ist durch neutrale Einträge.

Der Zustand 42 liegt vor, nachdem fünf verschiedene zweite Teilnehmer T2 bzw. Speicherkarten 50 mit dem Teilnehmer T1 bzw. einem Fahrtschreiber 51 in datenübertragenden Kontakt getreten sind. Demzufolge ist jeder Eintrag 31-35 nun gekennzeichnet durch ein anderes Datum, einen unterschiedlichen Sicherheitszertifikatsinhalt 52 und eine andere Erfassungszeit 53.

Der Zustand 43 stellt sich ein, nachdem ein zweiter Teilnehmer ursprünglich charakterisiert durch den Eintrag 33 zu einem späteren Zeitpunkt nochmals mit dem ersten Teilnehmer T1 in einen datenübertragenden Kontakt getreten ist. Demzufolge hat sich die Erfassungszeit 53 des Eintrages 33 aktualisiert.

Der Zustand 44 stellt sich ein, wenn bereits eine der Obergrenze an Einträgen 31-35 entsprechende Anzahl jeweils auf Grund einer Verbindung mit einem zweiten Teilnehmer T2 deneutralisiert worden sind und ein weiterer, bisher noch nicht bekannter zweiter Teilnehmer T2 mit dem ersten Teilnehmer T1 in einen datenübertragenden Kontakt tritt. Der gemäß der Erfassungszeit 53 älteste Eintrag 31 ist erfindungsgemäß mit einem neuen Eintrag 36 überschrieben.

In analoger Weise wird der Eintrag 32 in Zustand 45 von einem Eintrag 37 ersetzt.

Zustand 46 stellt sich ein, wenn ein mit dem ursprünglichen Eintrag 31 korrespondierender zweiter Teilnehmer T2 nochmals mit dem ersten Teilnehmer T1 eine datenübertragende Verbindung eingeht. Auch hier wird der nunmehr älteste Eintrag 34 von dem Eintrag 31, der einem in Folge des Überschriebs aus Zustand 44 unbekannten zweiten Teilnehmer T2 zugeordnet ist, ersetzt.

Patentansprüche

1. Verfahren zur sicheren Datenübertragung zwischen einem ersten Teilnehmer (T1) und zweiten Teilnehmern (T2), insbesondere zwischen einem Fahrtschreiber (51) eines Nutzfahrzeuges und Speicherkarten (50) mit jeweils mindestens einem Datenspeicher, wobei der erste Teilnehmer (T1) einen Speicher (6, 22) aufweist, in welchem eine bestimmte Anzahl Einträge (31-35) gespeichert sind, jeweils umfassend Kennungen (4) und zu diesen zugeordnete Sicherheitszertifikate (Cert) zweiter Teilnehmer (T2) mit einer Erfassungszeit (53) des Sicherheitszertifikates (Cert), welches Verfahren umfasst, dass der erste Teilnehmer (T1) von dem zweiten Teilnehmer (T2) eine Kennung (4) einholt, der erste Teilnehmer (T1) diese Kennung (4) mit den in dem Speicher (6, 22) gespeicherten Kennungen (4) vergleicht,
wenn eine übereinstimmende Kennung (4) in dem Speicher (6, 22) gespeichert ist, das dieser Kennung (4) zugeordnete Sicherheitszertifikat (Cert) Basis für eine nachfolgende Datenübertragung ist und die Erfassungszeit (53) des Sicherheitszertifikates (Cert) auf eine aktuelle Systemzeit aktualisiert wird,
wenn keine übereinstimmende Kennung (4) in dem Speicher (6, 22) gespeichert ist, der erste Teilnehmer (T1) eine Sicherheitszertifikatsverifikation mit dem zweiten Teilnehmer (T2) durchführt und bei Verifizierung einen dem verifizierten Sicherheitszertifikat (Cert) entsprechenden Eintrag (31-35) mit aktueller Erfassungszeit (53) in dem Speicher (6, 22) speichert, wobei der Eintrag (31-35) mit dem ältesten Erfassungsdatum durch diesen neuen Eintrag (31-35) ersetzt wird, wenn die bestimmte Anzahl an Einträgen (31-35) schon erreicht war.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Kennung (4) ein öffentlicher Schlüssel eines RSA-Verfahrens des zweiten Teilnehmers (T2) ist.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eine nachfolgende Datenübertragung TDES-verschlüsselt erfolgt, wobei nach erfolgter Verifizierung der Sicherheitszertifikate (Cert) beide Teilnehmer (T1, T2) eine Zufallszahl (RND) verschlüsselt an den anderen Teilnehmer (T1, T2) übersenden und beide Teilnehmer (T1, T2) jeweils unabhängig voneinander mittels der beiden Zufallszahlen (RND) einen gemeinsamen Schlüssel (80) zur Datenübertragung unter Benutzung des selben Algorithmus bestimmen.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Verifikation des Sicherheitszertifikats (Cert) des ersten Teilnehmers (T1) durch den zweiten Teilnehmer (T2) und umgekehrt folgende n Schritte umfasst:
in einem ersten Schritt übersendet der zweite Teilnehmer (T2) dem ersten Teilnehmer (T1) ein erstes Sicherheitszertifikat (Cert.Lev.1), welches der zweite Teilnehmer (T2) unter Benutzung eines ersten öffentlichen Schlüssels einer Verifizierung unterzieht und hierbei einen zweiten öffentlichen Schlüssel ermittelt, resultiert die Verifizierung in Authentizität,
wird der erste Schritt unter Verwendung eines weiteren übersendeten Sicherheitszertifikats (Cert.Lev.1,2) und des im vorhergehenden Schritt ermittelten zweiten öffentlichen Schlüssels an Stelle des ersten öffentlichen Schlüssels (n-1)-fach wiederholt, wobei sich stets ein

neuer zweiter öffentlicher Schlüssel und ein Verifizierungsergebnis ergibt.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass n=3 ist.

FIG 1

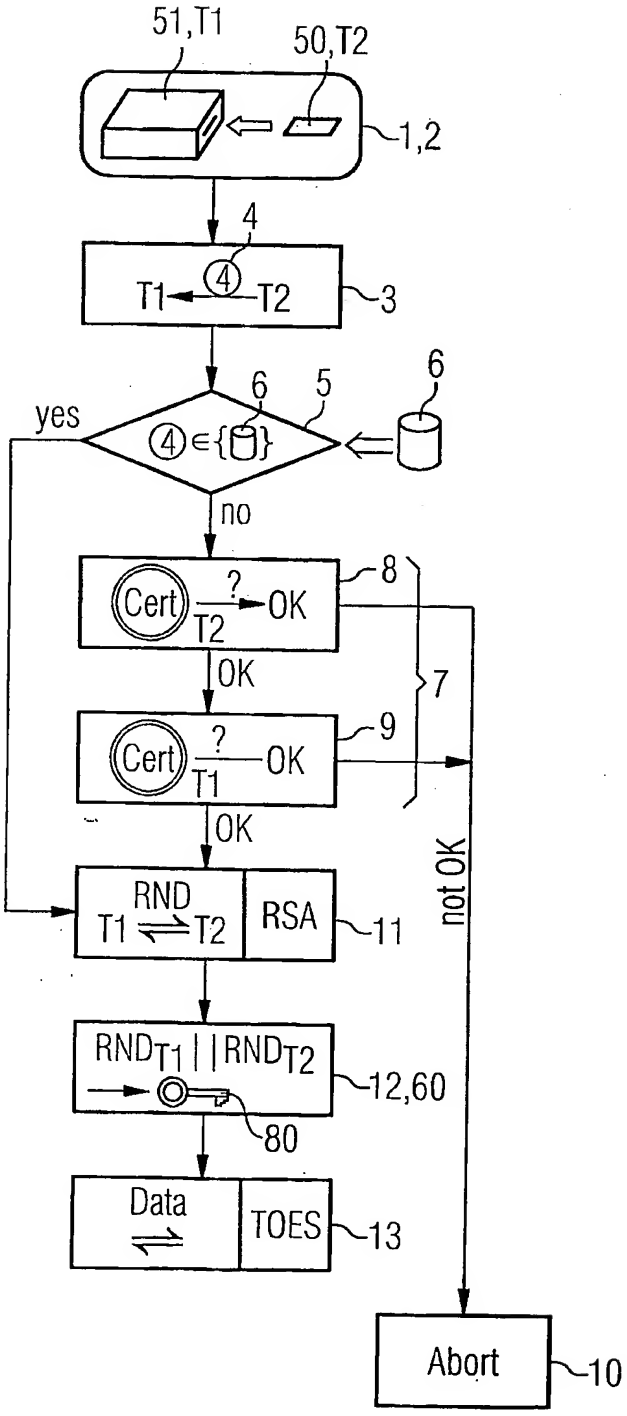

51,T1
50,T2
1,2
4
T1
④
T2
3
6
5
6
yes
④∈{}
no
Cert
?
T2
OK
8
OK
7
Cert
?
T1
OK
9
OK
not OK
RND
T1 ⇌ T2
RSA
11
RND T1 || RND T2
12,60
80
Data
⇌
TOES
13
Abort
10

FIG 2

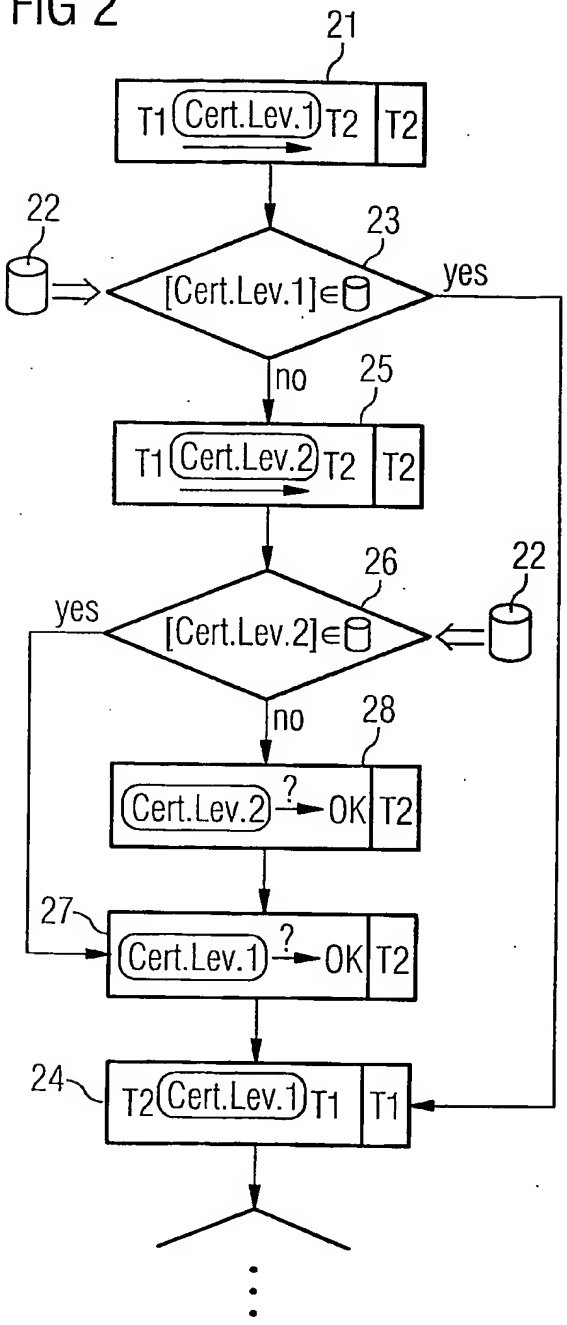

21
T1 Cert.Lev.1 T2 T2
22
23
[Cert.Lev.1]∈
yes
no
25
T1 Cert.Lev.2 T2 T2
26
22
yes
[Cert.Lev.2]∈
no
28
Cert.Lev.2 ? OK T2
27
Cert.Lev.1 ? OK T2
24
T2 Cert.Lev.1 T1 T1

FIG 3

Date Hex	CardContent	(...EOV | CHR...)		
0x00000000	...0x00000000	0x0000000000000000...	31	
0x00000000	...0x00000000	0x0000000000000000...	32	
0x00000000	...0x00000000	0x0000000000000000...	33	41
0x00000000	...0x00000000	0x0000000000000000...	34	
0x00000000	...0x00000000	0x0000000000000000...	35	

Date Hex	CardContent	(...EOV | CHR...)	(Date)	42
0x40346D00	...0x43B71B7F	0x0000000000000001...	(19.02.2004 08:00:00)	31
0x40347B10	...0x43B71B7F	0x0000000000000002...	(19.02.2004 09:00:00)	32
0x40348920	...0x43B71B7F	0x0000000000000003...	(19.02.2004 10:00:00)	33
0x40349730	...0x43B71B7F	0x0000000000000004...	(19.02.2004 11:00:00)	34
0x4034A540	...0x43B71B7F	0x0000000000000005...	(19.02.2004 12:00:00)	35

19.02.2004 15:00:00 — 43

Date Hex	CardContent	(...EOV | CHR...)	(Date)	
0x40346D00	...0x43B71B7F	0x0000000000000001...	(19.02.2004 08:00:00)	31
0x40347B10	...0x43B71B7F	0x0000000000000002...	(19.02.2004 09:00:00)	32
0x4034CF70	...0x43B71B7F	0x0000000000000003...	(19.02.2004 15:00:00)	33
0x40349730	...0x43B71B7F	0x0000000000000004...	(19.02.2004 11:00:00)	34
0x4034A540	...0x43B71B7F	0x0000000000000005...	(19.02.2004 12:00:00)	35

19.02.2004 16:00:00 — 44

Date Hex	CardContent	(...EOV | CHR...)	(Date)	
0x4034DD80	...0x43B71B7F	0x0000000000000006...	(19.02.2004 16:00:00)	36
0x40347B10	...0x43B71B7F	0x0000000000000002...	(19.02.2004 09:00:00)	32
0x4034CF70	...0x43B71B7F	0x0000000000000003...	(19.02.2004 15:00:00)	33
0x40349730	...0x43B71B7F	0x0000000000000004...	(19.02.2004 11:00:00)	34
0x4034A540	...0x43B71B7F	0x0000000000000005...	(19.02.2004 12:00:00)	35

19.02.2004 17:00:00 — 45

Date Hex	CardContent	(...EOV | CHR...)	(Date)	
0x4034DD80	...0x43B71B7F	0x0000000000000006...	(19.02.2004 16:00:00)	36
0x4034EB90	...0x43B71B7F	0x0000000000000007...	(19.02.2004 17:00:00)	37
0x4034CF70	...0x43B71B7F	0x0000000000000003...	(19.02.2004 15:00:00)	33
0x40349730	...0x43B71B7F	0x0000000000000004...	(19.02.2004 11:00:00)	34
0x4034A540	...0x43B71B7F	0x0000000000000005...	(19.02.2004 12:00:00)	35

19.02.2004 18:00:00 — 46

Date Hex	CardContent	(...EOV | CHR...)	(Date)
0x4034DD80	...0x43B71B7F	0x0000000000000006...	(19.02.2004 16:00:00)
0x4034EB90	...0x43B71B7F	0x0000000000000007...	(19.02.2004 17:00:00)
0x4034CF70	...0x43B71B7F	0x0000000000000003...	(19.02.2004 15:00:00)
0x4034F9A0	...0x43B71B7F	0x0000000000000001...	(19.02.2004 17:00:00)
0x4034A540	...0x43B71B7F	0x0000000000000005...	(19.02.2004 12:00:00)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/052530

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C5/08 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 102 10 320 A1 (INTERNATIONAL BUSINESS MACHINES CORP., ARMONK) 7 November 2002 (2002-11-07) paragraphs '0007! - '0027!, '0050!, '0051!; claims 2,5; figure 1	1-5
A	DE 198 43 424 A1 (FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V) 23 March 2000 (2000-03-23) column 7, line 21 - column 9, line 36; claims 4,17,18; figure 3	1-5
A	US 5 767 505 A (MERTENS ET AL) 16 June 1998 (1998-06-16) column 2, line 14 - column 4, line 16; claims 1,15; figure 2	1-5

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 August 2005	26/08/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Rüster, H-B

Form PCT/ISA/210 (second sheet) (January 2004)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	RANKL W ET AL: "AUTHENTISIERUNG" HANDBUCH DER CHIPKARTEN. AUFBAU - FUNKTIONSWEISE - EINSATZ VON SMART CARDS, MUNCHEN, CARL HANSER VERLAG, DE, 1996, pages 268-277, XP002127583 ISBN: 3-446-18893-2 pages 268-277	1-5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2005/052530

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 10210320 A1	07-11-2002	NONE	
DE 19843424 A1	23-03-2000	AT 225548 T	15-10-2002
		CA 2344429 A1	30-03-2000
		DE 59902963 D1	07-11-2002
		DK 1099197 T3	10-02-2003
		WO 0017826 A1	30-03-2000
		EP 1099197 A1	16-05-2001
		ES 2184500 T3	01-04-2003
		PT 1099197 T	28-02-2003
US 5767505 A	16-06-1998	DE 4402613 A1	03-08-1995
		AT 166474 T	15-06-1998
		AU 1704595 A	15-08-1995
		CZ 9602229 A3	13-11-1996
		WO 9520801 A1	03-08-1995
		DE 59502254 D1	25-06-1998
		DK 741891 T3	08-03-1999
		EP 0741891 A1	13-11-1996
		ES 2118568 T3	16-09-1998
		HU 74525 A2	28-01-1997
		NO 963058 A	23-07-1996
		PL 316842 A1	17-02-1997

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2005/052530

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07C5/08 G07F7/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07C G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 102 10 320 A1 (INTERNATIONAL BUSINESS MACHINES CORP., ARMONK) 7. November 2002 (2002-11-07) Absätze '0007! - '0027!, '0050!, '0051!; Ansprüche 2,5; Abbildung 1	1-5
A	DE 198 43 424 A1 (FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V) 23. März 2000 (2000-03-23) Spalte 7, Zeile 21 - Spalte 9, Zeile 36; Ansprüche 4,17,18; Abbildung 3	1-5
A	US 5 767 505 A (MERTENS ET AL) 16. Juni 1998 (1998-06-16) Spalte 2, Zeile 14 - Spalte 4, Zeile 16; Ansprüche 1,15; Abbildung 2	1-5

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann nahelegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
19. August 2005	26/08/2005

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Rüster, H-B

Formblatt PCT/ISA/210 (Blatt 2) (Januar 2004)

Internationales Aktenzeichen
PCT/EP2005/052530

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	RANKL W ET AL: "AUTHENTISIERUNG" HANDBUCH DER CHIPKARTEN. AUFBAU - FUNKTIONSWEISE - EINSATZ VON SMART CARDS, MUNCHEN, CARL HANSER VERLAG, DE, 1996, Seiten 268-277, XP002127583 ISBN: 3-446-18893-2 Seiten 268-277	1-5

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2005/052530

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
DE 10210320	A1	07-11-2002	KEINE		
DE 19843424	A1	23-03-2000	AT	225548 T	15-10-2002
			CA	2344429 A1	30-03-2000
			DE	59902963 D1	07-11-2002
			DK	1099197 T3	10-02-2003
			WO	0017826 A1	30-03-2000
			EP	1099197 A1	16-05-2001
			ES	2184500 T3	01-04-2003
			PT	1099197 T	28-02-2003
US 5767505	A	16-06-1998	DE	4402613 A1	03-08-1995
			AT	166474 T	15-06-1998
			AU	1704595 A	15-08-1995
			CZ	9602229 A3	13-11-1996
			WO	9520801 A1	03-08-1995
			DE	59502254 D1	25-06-1998
			DK	741891 T3	08-03-1999
			EP	0741891 A1	13-11-1996
			ES	2118568 T3	16-09-1998
			HU	74525 A2	28-01-1997
			NO	963058 A	23-07-1996
			PL	316842 A1	17-02-1997